



# UNITED STATES PATENT AND TRADEMARK OFFICE

50

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,146	06/20/2001	John E. Brezak	MS1-886US	5712
22801	7590	05/23/2005	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			KLINGER, SCOTT M	
			ART UNIT	PAPER NUMBER
			2153	

DATE MAILED: 05/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/886,146

Applicant(s)

BREZAK ET AL.

Examiner

Scott M. Klinger

Art Unit

2153

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 10 January 2005.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-35 and 38-61 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-35 and 38-61 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

Claims 1-35 and 38-61 are pending.

#### *Priority*

No claim for priority has been made. The effective filing date for subject matter in the application is 20 June 2001.

#### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-35, 38-46, 48-55, are 57-61 are rejected under 35 U.S.C. 102(b) as being anticipated by Fox et al. ("*Security on the Move: Indirect Authentication Using Kerberos*", 1996, hereinafter "*Fox*"). Fox discloses indirect authentication using kerberos. Fox shows,

In referring to claims 1, 3-5, 12, 16, 18-20, 26,28-30, 31, 33, 35

- identifying a target service to which access is sought on behalf of a client; and causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third party:

*"Charon interaction consists of two distinct phases: the handshake phase, in which the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase, in which the proxy accesses Kerberized services on the client's behalf. The Charon protocol module on the proxy and the Charon client-side software are responsible for the flow of control during both phases."* (Fox, page 157, paragraph 2)

Art Unit: 2153

the server provides the trusted third party with:

- a service credential authenticating the server, information about the target service, and a service credential previously provided by the client for the service, and wherein the client ticket includes implementation-specific identity information:

*“During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy. From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase.”* (Fox, page 157, paragraph 3)

In referring to claim 2, 17, 27, 32,

- The trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, A certificate granting authority service, and A domain controller service:

Fox Fig.1 shows the trusted third party includes a KDC

In referring to claim 6, 8, and 21,

- Causing the trusted third-party to verify that the client has authorized delegation:  
Verifying authorized delegation is inherently implied in a system that uses Kerberos

In referring to claims 7 and 22,

- The trusted third-party includes a key distribution center (KDC):  
Fox Fig.1 shows the trusted third party includes a KDC
- Causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a restriction placed on the ticket originating from the client:  
Verifying authorized delegation is inherently implied in a system that uses Kerberos

Art Unit: 2153

In referring to claim 9, 23, and 34,

- The server is a front-end server with respect to a back-end server that is coupled to the front-end server:  
The proxy is a front-end server with respect to the client
- The back-end server is configured to provide the target service to which access is sought.  
The target service is a back -end server with respect to the client

In referring to claims 10 and 24,

- The trusted third-party includes a key distribution center (KDC):  
Fox Fig.1 shows the trusted third party includes a KDC
- The KDC provides a ticket-granting-ticket associated with the client to the client; and the client does not provide the ticket granting ticket to the server:  
*“During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy.”* (Fox, page 157, paragraph 3)

In referring to claims 11 and 25,

- The trusted third-party includes a key distribution center (KDC):  
Fox Fig.1 shows the trusted third party includes a KDC
- The server requests the new credential in a ticket granting service request message that includes a service ticket provided by the client to the server:  
*“During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy.”* (Fox, page 157, paragraph 3)

In referring to claims 13, 14, and 15,

- The implementation-specific identity information includes information selected from a group comprising privilege attribute certificate (PAC) information, security identifier

Art Unit: 2153

information, Unix identifier information, Passport identifier information, certificate information:

The system of Fox contains security identifier information

In referring to claim 38,

- separately authenticating a server and a client; providing the client with a client ticket granting ticket and a service ticket for use with the server:

*“the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase”* (Fox, page 157, paragraph 2)

- providing the server with a server ticket granting ticket; providing the server with a new service ticket for use by the server for use with a new service without requiring the server to have access to the client ticket granting ticket:

*“During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy. From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase.”* (Fox, page 157, paragraph 3)

In referring to claim 39,

- Causing the server to request the new service ticket on behalf of the client by forwarding the server ticket granting ticket, information identifying the new service, and the service ticket to a trusted third party:

*“During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy. From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase.”* (Fox, page 157, paragraph 3)

Art Unit: 2153

In referring to claims 40, 48, 49, 57, and 58,

- Identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;  
*“the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase”* (Fox, page 157, paragraph 2)
- Causing a server that is operatively coupled to the target service and the client to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication protocol:
- The server communicates with the client via the first authentication protocol which inherently implies identifying the client and the first authentication protocol
- Causing the server to request a new service credential, for use by the server and the target service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and the service credential to itself.

*“Charon interaction consists of two distinct phases: the handshake phase, in which the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase, in which the proxy accesses Kerberized services on the client’s behalf. The Charon protocol module on the proxy and the Charon client-side software are responsible for the flow of control during both phases.”* (Fox, page 157, paragraph 2)

In referring to claims 40 and 50,

- The second authentication method trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service:

Fox Fig.1 shows the trusted third party includes a KDC

Art Unit: 2153

In referring to claims 42, 51, and 59,

- The new service credential is granted in an identity of the client rather than an identity of the server:

*“During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy.”* (Fox, page 157, paragraph 3)

In referring to claims 43, 52, and 60,

- The service credential is configured for use by the server and the target service to which access is sought.

*“From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase.”* (Fox, page 157, paragraph 3)

In referring to claims 44, 53, and 61,

- The credential authenticating the server includes a ticket granting ticket associated with the server.

*“From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase.”* (Fox, page 157, paragraph 3)

In referring to claims 45 and 54,

- Upon receiving a request for the new service credential from the server, causing the second authentication method trusted third-party to verify that the client has authorized delegation:

Verifying authorized delegation is inherently implied in a system that uses Kerberos

In referring to claims 46 and 55,

- The server is a front-end server with respect to a back-end server that is coupled to the front-end server;



Art Unit: 2153

The proxy is a front-end server with respect to the client

- The back-end server is configured to provide the target service.

The target service is a back -end server with respect to the client

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 47 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox in view of Freier et al. ("*The SSL Protocol Version 3.0*", 18 Nov 1996, hereinafter "*Freier*"). Although Fox shows substantial features of the claimed invention, Fox does not show using SSL as the first authentication method. Nonetheless this feature is well known in the art and would have been an obvious modification to the system disclosed by Fox as evidenced by Freier.

In analogous art, Freier discloses SSL version 3.0. Freier shows SSL can be used to provide communication privacy over the Internet.

Given these teachings, a person of ordinary skill in the art would have readily recognized the desirability and advantages of modifying the system of Fox so as to use SSL, such as taught by Freier, in order to provide security for applications that don't support Kerberos authentication (For example, Outlook and Netscape email clients).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott M. Klinger whose telephone number is (571) 272-3955. The examiner can normally be reached on M-F 9:00am - 5:30pm.

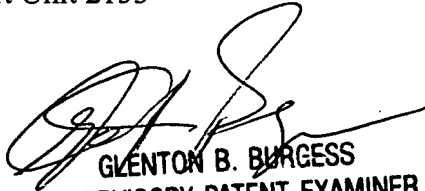
Art Unit: 2153

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on (571) 272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Scott M. Klinger  
Examiner  
Art Unit 2153

smk



GLENTON B. BURGESS  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100